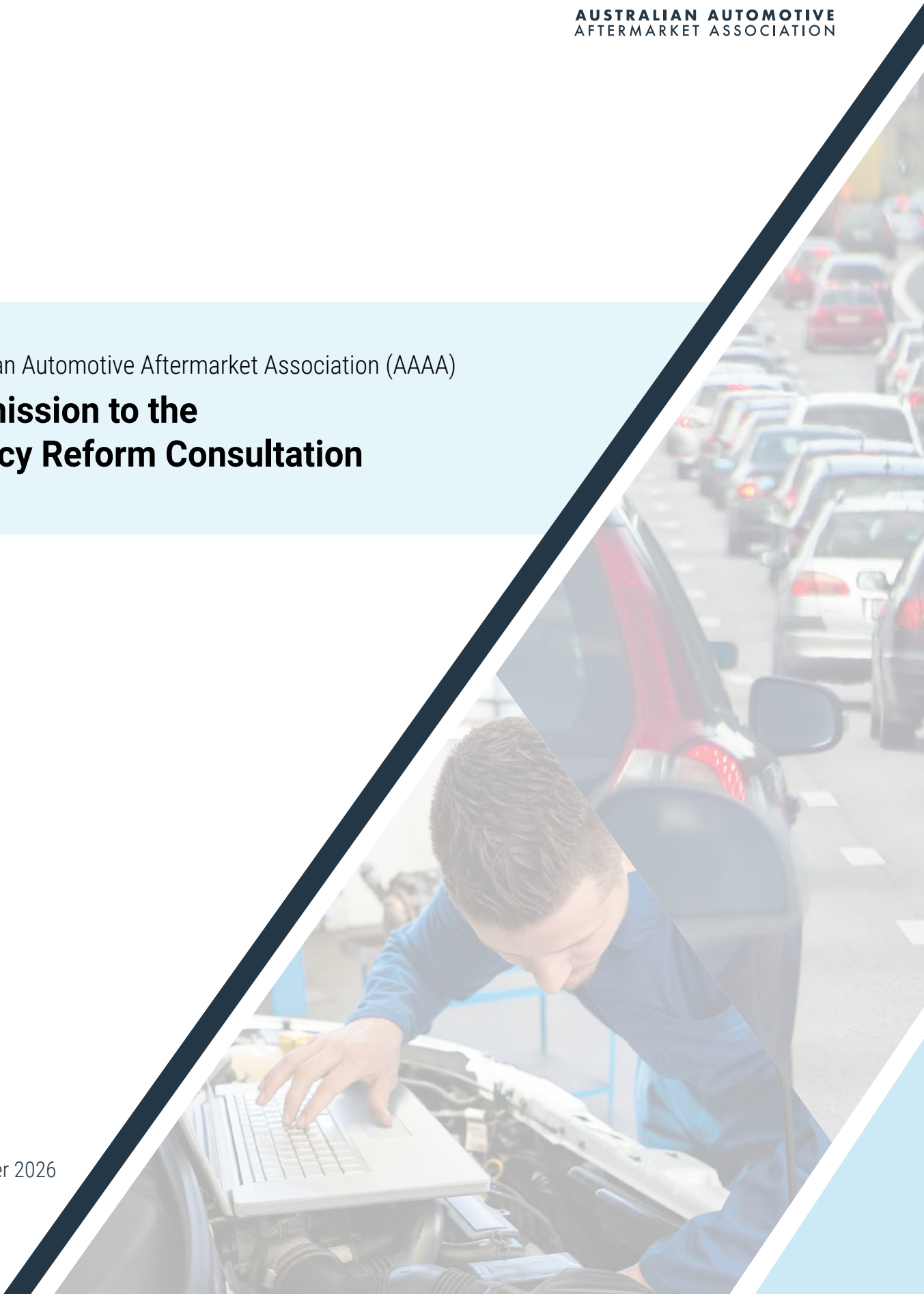
AUSTRALIAN AUTOMOTIVE
AFTERMARKET ASSOCIATION

Australian Automotive Aftermarket Association (AAAA)

# Submission to the Privacy Reform Consultation



September 2026

# Contents



## FOR FURTHER INFORMATION

Lesley Yates
Director Government Relations and Advocacy
Australian Automotive Aftermarket Association
lyates@aaaa.com.au

AAAA National Office
7 – 8 Bastow Place,
Mulgrave VIC 3170
Ph: 03 9545 3333

**www.aaaa.com.au**

# About the AAAA

The Australian Automotive Aftermarket Association represents businesses operating across the Australian automotive aftermarket, including manufacturers, distributors, retailers, service and repair businesses, and specialist automotive service providers. Our members diagnose, maintain, repair and modify vehicles throughout their working lives.

Connected vehicle data is increasingly important to safe and effective diagnosis, maintenance and repair. It also creates significant privacy risks because modern vehicles can generate information about a person's movements, behaviour, communications and daily routines. Privacy reform must protect individuals while preserving their ability to direct relevant vehicle data to the repairer or service provider of their choice.

# Executive Summary

AAAA supports the Government's objective of strengthening Australia's privacy framework. The Exposure Draft improves the definitions of personal information, collection, consent and disclosure, introduces a fair and reasonable handling test, and recognises precise geolocation tracking data as sensitive information. These reforms provide a stronger foundation for regulating connected vehicle data.

The Exposure Draft does not, however, provide adequate protection for drivers, passengers and other users of connected vehicles. Most vehicle-generated personal information could still be collected without affirmative consent. The proposed geolocation definition is narrow, notification obligations do not guarantee that every vehicle user is informed, and the new right to erasure is limited to large digital platforms. The Bill also lacks clear rules for secondary uses of vehicle data, including insurance assessment, consumer profiling, marketing and other decisions that may materially affect individuals.

The consultation paper identifies connected vehicles as an emerging technology but does not examine their specific privacy risks or ask targeted questions about them. This is a material omission. A vehicle is a mobile, sensor-rich data platform that may be used by several people and remain in service through multiple owners. A privacy model based largely on the relationship between a digital service and a single account holder does not address that environment.

AAAA recommends that the final reform package include connected vehicle provisions or provide for an enforceable connected vehicle privacy code. The framework should require express and separate consent for non-essential collection, meaningful in-vehicle notice and controls, rights of access and deletion, safeguards for secondary drivers and passengers, and strict rules for disclosure to insurers, data brokers, advertisers and consumer reporting bodies. It must also protect a consumer's right to authorise secure access by their chosen repairer or automotive data intermediary.

# Recommendations

| | | |
|---|---|---|
| 1 | **Connected vehicle rules** | Include specific connected vehicle provisions in the legislation or require the development of an enforceable connected vehicle privacy code. |
| 2 | **Express consent** | Require affirmative, express and purpose-specific consent before collecting vehicle-generated personal information that is not strictly necessary for immediate safety, operation, diagnosis, repair, an emergency response or another service expressly requested by the individual. |
| 3 | **Broader location protection** | Protect vehicle-derived location and journey information whenever it is reasonably capable of revealing an individual's movements, routines or destinations. Protection should not depend solely on a 500-metre threshold or the information being held over time. |
| 4 | **In-vehicle transparency** | Require clear notice through the vehicle and any connected application, together with a simple privacy dashboard showing the categories collected, purposes, recipients, retention periods and available controls. |
| 5 | **Rights for all vehicle users** | Ensure that protections apply to drivers, passengers, employees, renters, borrowers and subsequent owners. Consent from the purchaser or account holder should not be treated as consent from every person using the vehicle. |

| | | |
|---|---|---|
| **6** | **Access, deletion and disabling** | Give individuals a practical right to access, correct, download and delete connected vehicle data, and to disable non-essential collection. These rights should apply to manufacturers, telematics providers and other entities that control the information, not only large digital platforms. |
| **7** | **Restrictions on harmful secondary use** | Require express consent for disclosure to insurers, consumer reporting bodies, data brokers and advertisers, and for uses that may affect insurance, credit, employment, warranty or access to services. |
| **8** | **Consumer-directed repair access** | Confirm that privacy protections support a consumer's right to authorise secure, purpose-limited access to necessary vehicle data by a repairer or intermediary of their choice. |
| **9** | **Vehicle lifecycle controls** | Require effective de-provisioning, account transfer, data deletion and privacy resets when vehicles are sold, leased, rented, returned or transferred between fleet users. |
| **10** | **Accountability across the data chain** | Require clear allocation of responsibility, auditable access records, retention limits and privacy-by-design systems across manufacturers, dealers, telematics providers, processors and other recipients. |

# Connected vehicles require specific treatment

Connected vehicles routinely communicate with manufacturers, telematics providers and other service providers. Depending on the vehicle and services enabled, this can involve information generated by vehicle systems, information entered by users and information transferred from connected devices.

Information capable of being associated with an identifiable driver may include:

- precise and approximate location, routes, destinations and journey history
- speed, acceleration, braking, steering, time of travel and other driving behaviour
- odometer readings, vehicle use, charging activity, energy use and refuelling patterns
- diagnostic trouble codes, component condition, maintenance history and repair information
- vehicle, account, device and network identifiers
- contacts, call records, messages, media and other information copied or displayed through a paired device
- voice commands, cabin camera or microphone information, occupancy and biometric information where those systems are fitted
- inferences about a person's home, workplace, routines, health, religious activity, relationships, preferences or behaviour

Not every vehicle collects every category, and not every item will be personal information in every context. The relevant point is that connected vehicles can combine technical and behavioural data at a scale that allows an individual to be identified, singled out or assessed. The Bill's expanded definition of personal information is therefore important, but coverage alone does not provide effective control.

# Assessment of the Exposure Draft

### Expanded definitions provide a stronger foundation

The proposed definition of personal information expressly recognises identifiers, location information, characteristics, behaviour, preferences and patterns of activity. It also recognises that a person may be reasonably identifiable by combining information with other information reasonably available to the entity. These provisions should capture vehicle data linked through a vehicle identification number, connected services account, mobile device or other identifier where it relates to an identifiable driver.

The amended definition of collection is also helpful because it includes information generated or derived through an entity's own systems, observations, measurements or analytical processes. This should capture driving scores, risk profiles and other inferences produced from raw vehicle telemetry.

### Consent remains limited

The principal weakness is that the Exposure Draft does not require consent for the collection of personal information generally. APP 3 would permit collection, use and disclosure where the practice is lawful and fair and reasonable in the circumstances. Consent is required for sensitive information and for trading personal information, subject to exceptions.

As a result, a manufacturer may be able to collect extensive driving behaviour, vehicle-use, diagnostic, account and device information without affirmative consent. The information may be personal and highly revealing without meeting the statutory definition of sensitive information. Whether the practice is fair and reasonable would then depend on a broad, multi-factor assessment undertaken after the system and commercial arrangements have been designed.

For connected vehicles, the legislation should identify a limited category of data that may be collected without consent because it is strictly necessary for immediate vehicle operation, safety, diagnosis, repair or emergency response. Collection beyond those purposes should require affirmative, express and separate consent. A person who refuses optional data collection should not lose the ordinary safety, operation or repair functionality of the vehicle.

### The geolocation definition is too narrow

The inclusion of precise geolocation tracking data as sensitive information is welcome. However, the proposed definition requires location within a radius of 500 metres and collection and holding by reference to an individual's location over time.

Those thresholds may exclude information that remains highly revealing. A sequence of less precise locations can identify a home, workplace, medical service or place of worship. A single precise destination may expose sensitive circumstances even if the information is not retained as a longitudinal history. Protection should turn on what the information can reasonably reveal about an individual, not only its nominal precision or storage structure.

The treatment of derived sensitive information also requires care. Journey and destination data may disclose health, religion, political activity, trade union activity or intimate relationships before an entity formally records an inference in those terms. Entities should not avoid sensitive-information obligations by retaining the underlying data while choosing not to label the inference it plainly supports.

### Notification does not ensure awareness or choice

APP 5 would require an entity to take such steps, if any, as are reasonable to notify an individual of the fact and circumstances of collection and the intended purposes. The information must be clear, readily understandable, current and concise. These requirements improve the quality of notices but do not ensure that every affected individual receives one.

Connected vehicles are commonly used by people who did not purchase the vehicle, create the connected services account or receive the manufacturer's privacy notice. They include family members, employees, renters, borrowers, workshop staff and passengers. An account holder cannot consent on behalf of every person whose information the vehicle may collect.

The framework should require timely notice through the vehicle itself and any connected application. Where information is collected about a secondary driver or passenger, the vehicle should provide a practical guest mode or equivalent privacy control. Safety-critical warnings must remain clear and should not be crowded out by legal notices.

### Secondary use and disclosure need tighter controls

The consultation paper states that there would be no express requirement to obtain consent for unexpected or unrelated secondary uses and disclosures. These practices would instead be assessed under the fair and reasonable test. The proposed consent requirement for trading personal information is narrower than a general requirement for consent to share or repurpose it.

Vehicle data may pass among a manufacturer, connected services provider, dealer, technology supplier, analytics provider, insurer, fleet manager or other recipient. A disclosure may fall outside the definition of trade where no distinct payment is made for the information, where a processor acts for a controller, or where the disclosure forms part of providing a requested service. The fair and reasonable test remains relevant, but it does not give an individual a clear decision point before a consequential secondary use occurs.

The risk is demonstrated by regulatory action in the United States concerning General Motors and OnStar. In 2025, the United States Federal Trade Commission alleged that the companies collected precise geolocation and driving behaviour from millions of vehicles and sold it to consumer reporting agencies without adequate notice or affirmative consent. The information included hard braking, speeding and late-night driving and could be used in insurance decisions. The proposed order required affirmative express consent, access and deletion mechanisms, and an ability to limit certain collection. This provides a practical benchmark for Australian reform.

### Access and erasure rights are incomplete

The proposed right to erasure applies only to large digital platforms as defined by reference to categories in the Online Safety Act 2021. Vehicle manufacturers and telematics providers will not necessarily fall within that definition, even where they hold extensive and sensitive information about an individual's movements and behaviour.

APP 11 would require an entity to destroy or de-identify information when it is no longer needed, but it does not give a vehicle user a general right to request deletion. The entity retains substantial

control over whether it considers the information necessary for an available purpose.

The new access exception for technical impossibility or infeasibility also warrants caution. A connected vehicle system should be designed so personal information can be located, attributed, exported and deleted. An entity should not rely on technical infeasibility where reasonable privacy-by-design measures could have prevented the problem. Any exception should be narrow, independently reviewable and incapable of rewarding poor system design.

# Privacy and consumer choice in repair

Privacy protection and consumer choice in repair are complementary. Both require the individual, rather than the vehicle manufacturer, to control who may access information about their vehicle and for what purpose.

As diagnostic and service functions move from a physical vehicle port to remote and cloud-based systems, independent repairers may require access to data controlled by manufacturers or their service providers. Privacy should not be used to deny access to a repairer chosen by the consumer while allowing the manufacturer's own dealer network to use the same information.

The privacy framework should recognise a consumer-directed access pathway under which an individual can authorise a repairer or intermediary to obtain data reasonably necessary to diagnose, maintain or repair the vehicle. That pathway should include:

- clear and informed authorisation for the repair purpose
- access limited to the data and period reasonably necessary for that work
- secure authentication and transmission
- records showing what information was accessed and by whom
- the ability to revoke continuing access
- appropriate retention, security and deletion obligations for the recipient

This approach gives consumers genuine control without creating an exclusive data advantage for manufacturers. It also allows clear obligations to be applied to manufacturers, intermediaries and repair providers according to their roles.

# Responses to the emerging technology questions

## Updated definitions

### Question 1

**Are the proposed updated definitions sufficient to address the risks of emerging technologies?**

Partly. The definitions of personal information, collection, disclosure and reasonable identifiability are broad enough to capture much connected vehicle data. They should be supplemented by a vehicle-specific definition or examples covering telemetry, vehicle identifiers, driving behaviour, cabin data, data imported from paired devices and derived inferences. The definition of precise geolocation tracking data should also be broadened.

## Meaning of collection

### Question 2

**Is the definition of collection sufficiently flexible to capture information collected through new technologies?**

The inclusion of information generated or derived through systems, observations and measurements is appropriate and should capture vehicle-generated data and inferred profiles. The legislation should make clear that information is collected when a connected vehicle or associated system records or transmits it, including where the information initially relates to a vehicle but is reasonably capable of being linked to an individual.

## Meaningful consent

### Question 3

**To what extent can the reforms ensure that consent is meaningful where data capture is not transparent?**

The proposed consent definition is a sound starting point, but consent cannot be meaningful if it is sought through bundled terms at purchase, buried in an application or treated as a condition of ordinary vehicle use. Connected vehicles require separate choices by purpose, in-vehicle notice, simple settings, withdrawal mechanisms and continued access to essential vehicle functions when optional collection is declined.

## Remedies

### Question 4

**Are existing remedial options adequate?**

No. Individuals need rights to access, correct, export and delete connected vehicle data and to disable non-essential collection. The erasure right should not be limited to large digital platforms. Remedies should apply across the vehicle data chain and support complaints about inaccurate driving profiles or consequential decisions based on vehicle data.

## Compliance

### Question 5

**To what extent will the measures encourage improved compliance?**

The fair and reasonable test, improved definitions and stronger security obligations should improve compliance. Their effect will be limited unless connected vehicle expectations are made explicit. An enforceable code, clear OAIC guidance, privacy-by-design requirements and auditable consumer controls would give industry greater certainty and provide the regulator with practical standards against which conduct can be assessed.

# Proposed connected vehicle principles

| Principle | Required outcome |
|---|---|
| **Necessary collection** | Vehicle data should be collected without consent only where strictly necessary for immediate safety, operation, diagnosis, repair, an emergency response or another service expressly requested by the individual. |
| **Separate choice** | Optional collection and each materially different secondary purpose should require affirmative and unbundled consent that can be withdrawn as easily as it is given. |
| **Visible controls** | Every connected vehicle should provide clear, accessible controls showing what is collected, where it is sent and how the individual can stop non-essential collection. |
| **Rights across the chain** | Access, correction, portability and deletion rights should follow the information across manufacturers, dealers, service providers, processors and other recipients. |
| **Consumer-directed repair** | Individuals should be able to direct relevant vehicle data securely to the repairer or intermediary of their choice, subject to purpose limitation and security safeguards. |
| **Lifecycle protection** | Privacy settings and data should be securely reset or transferred when a vehicle changes owner, account holder, renter or fleet user. |
| **Accountable design** | Systems should be designed to identify, export, delete and audit personal information. Technical architecture should not defeat statutory rights. |

# Conclusion

The Exposure Draft would materially improve Australia's general privacy framework, but it does not yet provide an adequate response to connected vehicles. The combination of continuous data generation, opaque transmission, multiple users and potentially consequential secondary uses requires clearer statutory protection.

AAAA recommends that the Government address connected vehicles expressly in the final reform package and develop enforceable requirements with the automotive sector, consumer representatives, privacy experts and the independent repair industry. The final framework should give individuals real control over collection and disclosure while preserving their ability to authorise secure access for diagnosis, maintenance and repair.

AAAA welcomes further engagement with the inquiry and would be pleased to discuss the issues raised in this submission. For any questions relating to this submission, please contact the AAAA Director of Government Relations and Advocacy, Ms Lesley Yates (lyates@aaaa.com.au).

# References


1 Australian Government Attorney-General's Department, Privacy Amendment (Personal Data Protection) Bill 2026 Exposure Draft.

2 Australian Government Attorney-General's Department, Privacy Reform Consultation Paper, 2026.

3 United States Federal Trade Commission, FTC Takes Action Against General Motors for Sharing Drivers' Precise Location and Driving Behavior Data Without Consent, 16 January 2025.

AUSTRALIAN AUTOMOTIVE
AFTERMARKET ASSOCIATION